Check for updates

DOI: 10.1002/jsc.2411

RESEARCH ARTICLE

WILEY

From the internet of things toward the internet of bodies: Ethical and legal considerations

Moufid El-Khoury[1] | Cenk Lacin Arikan[2]

[1]College of Law, Notre Dame University (NDU), Notre Dame, Lebanon

[2]American University of the Middle East (AUM), College of Business Administration, Kuwait, Kuwait

Correspondence
Cenk Lacin Arikan, Abu Fatira, Block 2, Street 150, Building 575, Apartment 4, Kuwait.
Email: cenklacin.arikan@aum.edu.kw

Abstract

The proliferation of the internet of things makes the gray area of ethics darker and lighter simultaneously, and the law is currently not construed to accompany the steady progression toward the internet of bodies. The internet of things is challenging the traditional construct of ownership, and users are progressively losing control over their IoT devices. The internet of bodies is the awaiting new normal where human bodies and minds form a connected network pervaded by the Internet. The integrity of human bodies will rely more and more on the internet. In this context, the future calls for a balance between divergent interests of appealing technological progress and vital human safety.

KEYWORDS
internet of bodies, internet of everything, internet of things, machine-based decisions, potential capability

JEL CLASSIFICATION
K12, K20, K29, M10, M19, O33, O38.

1 | INTRODUCTION

Our human bodies and the things surrounding us are progressively merging with the internet's bits and bytes. The proliferation of the internet of things (IoT) and its progression toward the internet of bodies (IoB) present complex and new challenges for our society. Discrimination issues and the safeguard of privacy and security are among the challenging concerns awaiting the future hybrid society where the human body and mind become the new platform for technological innovation.

The constant proliferation of the IoT exacerbates the relativism of business ethics. The steady progression towards the IoB makes the gray color of ethics darker and lighter at the same time. Technological innovation and cognitive enhancement will undoubtedly clash with social imperatives such as the integrity and the physical safety of the human body. To apprehend this subtle yet visible progression, society as a whole will need to define the boundaries of business ethics of the "internet of everything." Despite the pressing need for guidelines and boundaries, the law is currently unprepared to remedy the social, economic, and physical harm this digital transformation may entail.

The purpose of this article is to shed light on the ever-growing progression from the IoT toward the IoB. The Article starts by depicting the IoT as the new normal. Then, some ethical and legal considerations of the IoT are examined. Finally, the article ends by exploring the IoB and discusses some of its challenges affecting our whole society.

2 | WHAT IS THE INTERNET OF THINGS?

The IoT is ubiquitous and already an overwhelming and pervasive reality. It is affecting our way of life significantly and shifting our traditional social and economic paradigms. IoT can be defined as everyone and everything being connected at all times through the internet network (Guillemin & Friessi, 2009; Haller, Karnouskos, & Schroth, 2009). In other words, the IoT encompasses in its realm anyone and anything that is producing some type of data and is connected to the internet. Some authors have also called the "internet of things" the "internet of everything" (Peppet, 2014).

Various daily activities can serve as a helpful example. Suppose you are using your smartphone to set your alarm clock for tomorrow

 © 2021 John Wiley & Sons Ltd.

morning. In that case, IoT will enable the alarm function to integrate with the traffic data and determine if one should be waking up a little earlier or if one can afford to sleep a bit longer. In other words, the decision will be modified according to the parameters of the available data pertain. On the same day, after waking up and getting ready to leave for commuting to work, IoT will know how many people and who exactly is using that specific route. Therefore, one's navigation system will interact with others and be affected by traffic lights, traffic density, and traffic behaviors. As people leave work, IoT will know their weekly routines and notice any deviation instantly. It will interfere with any upcoming personal plan or schedule made depending on its integrated data-driven logic. Suppose a person decides to engage in any activity that might trigger any parameter IoT has already mapped out. In that case, that input will instantaneously be integrated for further personal decisions and actions. These examples reflect the nature and the potential capability IoT has over human lives.

The above examples point to relatively simple and daily activities where IoT will most likely improve the quality of life by enhancing the decision-making processes in which we engage. However, other cases offer different examples where IoT-based decisions are more critical and their effects more severe. In this context, the below questions naturally arise and point to uncertain and blurry horizons. For example, will IoT entail an overdose of hegemonic technology? Who or which institutions/organizations will control the design of governing parameters? How will the parameters be fed with new data? In data collection, how will informed consent be guaranteed and protected? In the event of a data breach, what mechanisms will ensure security? How will IoT evolve in time; through its artificial intelligence or a combination of human input and machine-based decisions (a hybrid structure)? What mechanisms will ensure optimum solutions and decisions? Who will define the optimum solutions and what will be their criteria? What will be the value system underlying the business decision-making? What about corporate liability in the context of IoT? Is the current legal court system the appropriate forum before which IoT users can seek recovery?

The above questions illustrate the uncertainty surrounding IoT and its use. It seems that none of these questions can be addressed with clear-cut answers. In this context, tackling the ethical and legal aspects of the IoT is today a pressing need to ensure an equitable and safe transition towards the awaiting reality of the IoB.

According to Popescul and Georgescu (2013), it is the use of some technologies embedded within the IoT that puts ethics at the heart of this new normal of constant connectedness. Firstly, "IoT is based on a global infrastructure network which uniquely connects physical and virtual objects, by exploiting the data captured by the sensors" (Popescul & Georgescu, 2013, p. 209). Therefore, there are two main issues at the forefront. On the one hand, any problem innate in the system is a global scale with no frontiers whatsoever. On the other hand, IoT embraces both physical and cyber entities. In other words, IoT goes beyond real physical infrastructure into computerized and software systems. The widening use of self-driving cars would be a good example. Even though such car systems are improving, no system provider can guarantee the system from being hacked.

Some of these technologies embedded in the IoT can be summarized as illustrated in this non-exclusive list: First, RFID (Radio Frequency Identification): These systems use electromagnetic fields that allow you to "tag" items, places, and even people. Second, sensors: These systems collect data on an ongoing basis, such as "proximity, temperature, ambient light, accelerometers" (Popescul & Georgescu, 2013, p. 209). Third, GPS (global positioning solutions): These solutions allow continuous localization of stationary or moving objects with very high precision. Fourth, 3G, 4G, and 5G: These different generations of mobile technology allow the transfer of data in voice, images, videos, and encryption with varying degrees of coverage and at different frequencies.These available technologies enable the continuous collection and transmission of data. Nevertheless, the generally overlooked issue is that these technologies will also generate sensor data continuously. Home devices, such as Amazon Echo, Alexa Device, Google Nest, or car applications, such as Mercedes Me, continuously monitor people and their surroundings. In other words, the reason these IoT devices can instantaneously interact resides in the fact that they are always active and constantly collecting and processing data.

3 | ETHICAL CONCERNS OF THE IOT

The IoT changes tremendously human lives, the process of decision-making and organizational life. In all of these aspects, the very nature of ethics makes ethical concerns more relevant and significant in a society submerged by IoT. Ethics are innately conscious based, relative, and subjective. What is ethically acceptable for some in the context of IoT and its use may be deemed unethical by others. Zhilla, Abou Daher, Arikan, and El-Khoury (2018) emphasize increasing unethical practices and their possible consequences in today's modern life. They argue that "the wrongdoings of organizations affect not only businesses but also the people, the environment and the society as a whole" (p. 39). In other words, with the IoT's advanced capabilities, the ethical issues at hand and their outcomes may be significantly magnified.

Botterman & Tallacchini, 2018 argue that privacy issues are among the most fundamental concerns to be addressed by promoting an ethical IoT by design. The highly pervasive nature of IoT makes it a borderless mechanism that feeds on data continuously. The authors claim that "complexity becomes even higher when attempting to determine which data are personal and which are not" (Botterman and Tallacchini (2018), p. 907). Such a divide is important because it points out the very fact that even the seemingly useful disclaimers may not provide the much-needed clarity as to the content of the data provided.

Nissenbaum (2015) argues that privacy should be context-based. In other words, issues about cultures, geographies, religions, regulations, and the like should be considered when deciding which data violate privacy. This issue is an ethical dilemma in and of itself. It will be challenging to find consensus on any of these ethical issues. Therefore, it is highly improbable to adhere to standard rules when dealing with the ethical assessment of data collection and processing. Since IoT is a gigantic sea of information where the

whole globe is the source for data, the actual processing of data and the inferences entailed by such data may very well happen in a different setting, whether it may be geographically or culturally different. Even in the same cultural, geographical, religious, or regulatory environments, privacy may be invaded more often than once by IoT devices.

Some argue that access to IoT systems should be given to people (Weber, 2013). Such granted open access to IoT infrastructure might seem beneficial at first. However, people may have no competence or experience with such available information. Moreover, the availability of such access may create a false premise in the minds of common people. Since access is readily granted, common people will think that everything must be in order. In a world where people have extremely little control over what they receive in their mobiles or other devices in terms of unsolicited messages and excessive web advertising, it may be too utopic to expect them to have access to IoT infrastructure and actually to figure out what is happening behind the doors. Nevertheless, democratization of available data in the long term may potentially open new gateways into a freer and more just world.

Other major ethical concerns in IoT include ultra-connectivity, autonomous behavior, difficult identification, incorporated intelligence, ambiguity, and control difficulties (Van den Hoven, 2013). These are all potentially problematic areas for IoT from an ethics perspective. Ultra-connectivity refers to the Big Data nature of IoT. As data flow seamlessly and are created continuously, all these data are available to other so-called smart devices. For example, a home device like Alexa will exchange information with the new smart TV, and both will stay active even in standby mode. In time, both devices will know the user's preferences, whether they may be about TV shows, general world views, or more specific and sensitive issues. Soon enough, such devices will offer the content they feel fit.

Of course, such content will feed the user's views and perceptions and vice versa. Autonomous behavior points to the hybrid nature IoT applications have. As machines and humans interact, IoT can take over many of the repetitive tasks we as human beings used to carry out. At first glance, such a change would sound very promising. However, when people are hit by autonomous cars or the driver is too late to correct a mistake a self-driving vehicle makes, then the outcomes may become too costly to bear. Difficult identification refers to each connected entity's uniqueness. In other words, when IoT processes data provided by a broken device in making a decision, it would be easy to identify the source of the malfunction. However, when billions of devices are interconnected, identification in itself becomes a challenging issue. The decision-making and its effectiveness are complicated to trace back to the source. Incorporated intelligence describes how human beings may outsource certain decisions entirely because they may rely too heavily on IoT. In this respect, the human potential may be blocked to a certain extent. Human beings may become overdependent on the benefits IoT has to offer. Ambiguity may be experienced as the boundaries between machines and the natural world become thinner as technology advances. With time, because of significant enhancements, people may find themselves talking to their house cleaning robots. Identity issues may arise when in the human mind, interactive devices replace natural objects. Control difficulties point to the decentralized decision-making intrinsic to IoT. Since billions of devices are already interconnected; naturally, the difficulties in exerting control are only expected to increase in the future.

Personal data, under the realm of IoT, become a commodity in and of itself. In other words, personal data are no longer truly personal. Loewenthal (2014) emphasizes that data collection may not be conducted appropriately. Surveillance may have positive outcomes in preventing fraud or crime. Nevertheless, the collection of data remains very controversial. In this context, data gathering's ethical assessment remains a fundamental ethical dilemma IoT ethics should address.

In light of ethical considerations IoT entails, the most important question seems to center around the following: "who will own these data and knowledge, and who will use them and for what purpose?" (Kobayashi, Quilici-Gonzalez, Broens, & Quilici-Gonzalez, 2016, p. 89). Of course, the answer is not clear. Moreover, due to IoT's nature, even if there was a deliberate answer addressing these fundamental issues, uncertainties will remain. For example, home devices like Alexa may be regarded as listening devices intruding on consumers' privacy (Carey, 2018). However, Amazon may not necessarily be guilty of any wrongdoing. The nature of the IoT makes not quite evident the ethics surrounding IoT systems unless wrongdoing is established.

4 | THE END OF OWNERSHIP IN THE IOT ERA

Ownership as a legal construct is being affected by the digital world pervaded by the IoT. A corporation that markets IoT devices exerts significant control over the product, and yet the same corporation limits to a considerable extent what a consumer can do with the device in ways that, 20 years ago, would have appeared outrageous. For instance, we cannot own a coffeemaker that refuses to brew any unlicensed coffee. Fellmeth and Kheschtchin-Kamel (2019, p. 400) observe that "[t]oday, corporate control over consumer belongings is becoming the new normal."

Gilmore (1974) announced "The Death of Contract." The author argued that so many exceptions undermine consent, its objective manifestations, and the binding character of contractual obligations that the law of contracts is progressively fading away as a separate body of law. Perzanowshi and Schultz (2016) claim "The end of Ownership" in the digital age. In their work, the authors describe a fundamental paradigm shift in the personal property rights attached to the things we "own."

The issue of ownership in the context of IoT devices is two-fold. On the one hand, there is the ownership of the physical device that the customer would "buy." On the other hand, data ownership is generated by the use of such a device.

4.1 | The "ownership" of the IoT device

A customer who purchases an IoT device may not have the right to lend, resell, modify, or even repair the thing s/he owns. In this case,

the IoT companies are merely "licensing" IoT devices. The "sale agreement" is instead a "license agreement" that would limit to a considerable extent the peaceful enjoyment an actual "owner" would have. In the IoT era, the purchaser practically becomes a licensee who lacks the traditional property rights derived from ownership (Fellmeth & Kheschtchin-Kamel, 2019). In this regard, Determann and Fellmeth (2001, p. 20) argue that a "licensee" cannot be a separate consumer category. A consumer can either own personal property or rent it. A consumer does not buy or acquire an IoT device by concluding a "license agreement" where the ownership rights might be significantly disabled.

Schultz (2016, p. 37) claims that IoT manufacturers and distributors "are quietly attempting to shift the rules of ownership.". Some End User License Agreements (EULAs) provide that we do not "own" the product we "buy." These EULAs might deem illegal the act of repairing the IoT device by anyone other than the original manufacturer. When items were purely mechanical, the enjoyment of personal property was complete. In the IoT era, the device's software restricts the full enjoyment derived from the property right.

A notable example is the iconic John Deere tractor. John Deere "interposed" software between farmers and their tractors and claimed such software ownership. The farmers merely had "an implied license for the life of the vehicle to operate the vehicle" (Schultz 2016, p. 37).

4.2 | The "ownership" of the data generated by IoT devices

One could argue that the customer "owns" the sensor data produced by using the device (Elvy, 2018). However, despite a potential right of consumers in the data they generate, "buyers" frequently allow sensor data by the IoT companies in the EULAs they accept.

In this regard, Peppet (2014) observed that IoT devices' privacy policies are often silent about the ownership of sensor data generated by the device. When these policies address the issue of data ownership, the terms and conditions explicitly grant "ownership" to the manufacturer (Peppet, 2014, p. 145). Practically, the privacy policies principle is that the data generated by consumers' bodies, homes, smartphones, cars, and the like are "owned" by the manufacturer and not the consumers who generate them (Peppet, 2014, p. 163).

According to Rens (2019), the United States courts have tended to uphold and enforce the terms of the EULAs. Nevertheless, under these agreements, the bargain might lack informed consent and equitable exchange between the IoT company and the "buyer." The consumer might be consenting to the collection, storage, and processing of data not only by the seller company but also by third-party service providers. The buyer would give the IoT company the right to share the data with third-party vendors. These third parties might claim an interest in the data they store or process on behalf of IoT companies. This event will depend on the terms of the service agreements signed between the IoT company and these third-party service providers (Elvy, 2018).

The data centers and third parties might be located within or outside the buyer's country of residence. In other words, the buyer might be agreeing under the EULA to an international transfer and processing of data. Elvy (2018, p. 466) notes that "[t]hrough this consent, consumers could be said to grant or authorize IoT companies to obtain rights in the data they generate, including the right to process, aggregate, anonymize, and transform the data". What is more egregious is that these rights are frequently granted by the buyer without informed consent as a "royalty-free license" to use the generated data.

Practically, IoT companies are being granted under the EULAs proprietary rights in data sold as a commodity on the market. In this context, customer databases and lists could arguably be perceived as owned by IoT companies and subject to "legal assignment" (Elvy, 2018, p. 467). When an IoT company goes bankrupt, it may decide to sell the data it already possessed. Perceived as a commodity owned by the company, customer databases would be a part of the IoT company's "estate" when bankruptcy proceedings are initiated (Elvy, 2018, p. 473).

The legal protection that might be recognized as "personal information" such as the name, email, or address does not automatically apply to the sensor data generated by our connected devices at home. It might be uncertain whether the data generated by a sensor installed into the IoT device constitute "personal information" under the applicable law. The lack of a global legal framework worsens ambiguity and legal uncertainty. The definition of "personal information" differs from region to region. For instance, "personal information" or "personally identifiable information" do not have the same legal definition under US law or the European General Data Protection Regulation (GDPR). Furthermore, the company offering the IoT device on the market can contractually define what constitutes "personally identifiable information" (Peppet, 2014, p. 157) in its terms of use.

The IoT phenomenon is not only undermining the traditional personal property rights, but it is also eroding the economic value of the device supposedly "owned" by the customer. For example, a relatively old iPhone model will lose its economic value if its software updates and applications become outdated. In this case, the buyer may be left with a useless device. Rens (2019, p. 25) notes that "[t]he IoT is marked by a new development: remote control obsolescence". Remote-controlled obsolescence will render the IoT device obsolete "at the caprice" of the manufacturer or its successor. By nature, the IoT device relies on software and networked-based services. An IoT device's longevity and functionality will depend on the updates of reliable software and service providers' networks.

5 | WHO IS LIABLE WHEN IOT DEVICES CAUSE HARM TO IOT USERS?

The proliferation of IoT will undoubtedly increase the adjudication of harm that a malfunctioning IoT device may cause. It is no longer science fiction to be killed by a machine. Software bugs and errors have already been "implicated in deadly medical failures" (Matwyshyn, 2019, p. 140).

In this context, liability is more difficult to apprehend because various actors interfere in the manufacturing of an IoT device. Frequently, different companies worldwide design, build and assemble the different components that would constitute the final IoT product

(Siegel, 2020). Additional actors would also be involved in the collection and the processing of the data. IoT companies can recourse to a cloud computing company to manage their "burdensome IT infrastructure" (Siegel, 2020, p. 196). Any security breach at this level might directly impact the data related to consumers using IoT devices. Liability should also take into account the "standard of care" or the negligence of the cloud service provider. Given the number of variables involved in the manufacturing and functioning of an IoT device, the causation between the user's harm and the "alleged" fault of the manufacturer would be complicated to establish in court.

5.1 | IoT users may lack standing to seek relief before courts

The plaintiff in both civil and common law jurisdictions should establish standing to seek relief before a court. The principles governing standing will differ according to the procedural rules applicable before the court where the claim is brought. In general terms, a plaintiff has standing when he or she has suffered an "injury in fact" and can establish a causal connection between the harm suffered and the claim sought. A critical case before the US Supreme Court highlights the difficulty for plaintiffs to establish standing before courts. In the renowned *Clapper* case, some domestic US entities, including human rights, labor, legal, and media organizations, sought to declare unconstitutional a section added to the US Foreign Intelligence Surveillance Act (FISA) in 2008. The 2008 amendment allows government officials to acquire foreign intelligence information by intercepting foreign individuals' communications who are reasonably believed to be located outside the United States. Before the US Supreme Court, the issue was whether these domestic entities have legal standing to challenge the constitutionality of the FISA. The Supreme Court of the United States held in *Clapper v. Amnesty Int'l USA*[1] that to establish standing, "[…]an injury must be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling".[2] In the *Clapper* case, the US Supreme Court concluded that these domestic entities might have taken significant and costly measures to protect confidential communications' privacy. However, these preventive measures seek to protect a more hypothetical future injury and would not constitute an "injury-in-fact" that would satisfy the standing requirement.[3]

In this context, IoT users who are seeking to hold a company liable for a data breach resulting from a cyberattack may not have standing in court because it might be difficult for the plaintiff to prove an "injury-in-fact" that would be concrete, actual, and fairly traceable to the data breach.

5.2 | Substantive law might not be in favor of IoT users

Siegel (2020, p. 191) asserts that "[f]rom a purely legal cause of action perspective, there is not a single tried and tested, a successful legal theory that consumers can rely on to bring a cause of action against an IoT manufacturer". Under the traditional tort theory, a user's chance to succeed is weakened by the lack of a widely recognized definition of negligence for IoT manufacturers. The "standard of care" (Siegel 2020, p. 193) that an IoT company would need to abide by is unclear and yet to be defined. Furthermore, most of the EULAs accepted by the buyer at the time of the purchase bar tort liability through contractual "liability disclaimers" (Siegel 2020, p. 210).

Under a breach of contract claim, it might be difficult for the user to succeed without proving that s/he suffered actual monetary damages (Siegel, 2020). Nevertheless, some plaintiffs succeeded by claiming "unjust enrichment" (Siegel 2020, p. 209). Unjust enrichment is a legal concept based on equity. This claim would only require the proof of an unjust benefit conferred by the "buyer" upon the IoT defendant. Furthermore, the buyer of an IoT device can invoke contractual unconscionability, which is a legal construct based on procedural or substantive unfairness in forming the contract. For example, unequal bargaining power or surprises resulting from obscure language hidden in small print can constitute procedural unconscionability. Substantive unconscionability would refer to cases where the plaintiff establishes that the contract's substantive terms are "being one-sided or overly harsh" (Kirtley & Memmel, 2018, p. 508). In this regard, one could argue that the terms of the EULAs which grant IoT companies a worldwide free license to collect, process, use, and sell consumer-generated data are unconscionable.

6 | LEGAL CONSIDERATIONS OF IOT CYBERSECURITY

The very nature of IoT devices involves different physical infrastructures. When a farmer purchased a traditional and purely mechanical tractor, security was a physical concern directly related, such as the maneuvering of the vehicle or the engine's mechanical misfunctioning. Today, when a farmer purchases a 2020 high-end agricultural tractor, security is physical and remotely related to the software embedded within the engine and the data generated by this tractor. The IoT produces a paradigm shift like security itself. IoT devices make security a remote concern. For example, frequently IoT companies seek cloud service provider's services. Cloud storage services involve remote servers that would store and process data in different places using "different cloud computing models" (Schwartz, 2018, p. 1689). According to Kirtley and Memmel (2018, p. 461), such "splitting control" exacerbates the security of the IoT device purchased by consumers.

One of the most significant crises an IoT company might face is a cyberattack. A cyberattack might trigger specific legal obligations for the company. One legal question an IoT company should ask is whether it has a legal obligation to disclose and notify its customers of the data breach. The answer to this question will depend on the applicable laws governing data breaches. For instance, data breach notification laws can impose on IoT companies an obligation to maintain reasonable security measures and protect personal information

(Buttrick, Davidson, & McGowan, 2016). In the event of a data breach, the IoT company can also be required to provide some type of notification to the consumer. The IoT company might also be required by law to report the breach to local authorities, regulators, or administrative agencies.

From a consumer perspective, another legal question is related to the available legal remedies if private information is compromised as a result of the breach. In this context, the obligation to establish reasonable security measures might be difficult to challenge in legal proceedings because the technological capabilities are difficult to assess, and "the industry standards greatly complicate the development of workable standards of care" (Meglio, 2020, p. 1236). Furthermore, seeking relief is very difficult in the event of a data breach because the plaintiff might need to prove that the compromised data fall within the category of "personal information" as defined under the applicable law. Even if the plaintiff established the harm, the causation element required for recovery might be difficult to ascertain especially when there is a concurrent event that would have compromised the same personal information. For instance, it would be "nearly impossible" to prove that "the suffered identity theft was solely the result of the defendant's breach" (Buttrick et al., 2016, p. 22).

A recent example illustrates very well the legal implications cybersecurity can trigger in the context of IoT. Zoom Video Communications Inc. (Zoom) witnessed a significant increase in its users during the Covid-19 confinement period. Such a sudden increase revealed security flaws and privacy concerns which led a group of consumers to file class actions against Zoom before US courts. The plaintiffs claimed that Zoom misrepresented and breached its promise to provide the privacy and security it promoted among various allegations.[4] For instance, Zoom did not allegedly install the security encryption it was marketing on its website. Besides, some complaints contended that Zoom shared personal data with third parties such as LinkedIn and Facebook without obtaining the prior informed consent of Zoom's users.[5] Other complaints claimed that Zoom was faulted when it did not disclose the security flaws affecting its platform in a timely fashion. In this respect, investors alleged that Zoom made false and misleading public statements and did not knowingly reveal material and adverse facts that would affect the value of Zoom's stock on the financial markets.[6]

7 | FROM THE "INTERNET OF THINGS" TO THE "INTERNET OF BODIES"

The current state of technology reveals an ongoing progression of the IoT into a network of human bodies called the "Internet of Bodies" (Matwyshyn, 2019). The IoT's ethical and legal concerns become more pressing when our human bodies' integrity and functionality rely on the Internet and related technologies. Suppose the IoT undermines the ownership and enjoyment of a "buyer" or might cause sensitive information disclosure. In that case, the IoB can physically cause harm to individuals and may affect the integrity of the human mind and body directly. A simple fact such as poor Internet connectivity might physically affect the safety and health of IoB users who would rely on "life-enabling or hardwired IoB technologies" (Matwyshyn, 2019, p. 137).

Matwyshyn (2019) classifies IoB devices into three generations: Body External, Body Internal, and Body Melded. Body External devices include regulated "medical devices," unregulated "low risk" IoB devices related to general wellness and healthy lifestyle, and the non-health-related products such as educational and recreational connected "body-attached" devices (Matwyshyn, 2019, p. 95). Examples of Body External products are Internet-enabled robotic surgery machines, prosthetics connected to a mobile application, and smartwatches promoting and monitoring a healthy lifestyle. Another fascinating example is the "brain sensing headbands" (Matwyshyn, 2019, p. 96) used in the classroom to monitor student attention.

Body Internal devices refer to IoB devices that reside inside the human body or access the body "by breaking the skin" (Matwyshyn, 2019, p. 103). Some examples would be the pacemakers with digital components, cochlear implants with a Bluetooth feature, digital pills, sensor-enabled sutures, or the chips with cameras used during medical surgery.

Body Melded devices are those IoB devices that are integrated into the human mind with the Internet and technology. Besides the technical pitfalls, continuous connectedness potentially raises complex challenges both in terms of law and ethics. IoB devices affect brain-computer interfaces and might "extend and externalize portions of the human mind" (Matwyshyn, 2019, p. 112). The ambition of the body Melded devices lies in the utopic merging of biological intelligence with machine intelligence by connecting computers directly to the human brain. Today, these devices are mostly confined to cognitive enhancement research and medical treatment. For example, connected brain prosthetic devices are being used for treating Alzheimer's, Parkinson's, or Epilepsy patients. Yet, the "slippage into nonmedical uses of third-generation IoB is already visible" (Matwyshyn, 2019, p. 114).

When assessing the future corporate software liability and the IoB, Matwyshyn (2019, p. 139) predicts that courts will struggle "with fact-intensive legal inquiries in IoB". For instance, the variety of IoB factors that might affect the constitutive elements makes the legal remedy very specific to the unique facts of the case at hand. These facts will be dictated by complex relationships existing between the code, the software, the manufacturer, the developer, the internet provider, the cloud service provider, the seller of the IoB device, the third-party monitoring the use of such device, and finally, the conduct of an IoB user. Courts will be applying and elaborating on different legal theories and rules. Legal uncertainty will prevail when assessing and dealing with IoB devices. To take only the US market as an example, the fact-intensive legal inquiry surrounding the IoB will cause a "substantial variability within the national market" (Matwyshyn, 2019, p. 139). This fact-intensive characteristic of IoB litigation had already led to inconsistent legal decisions when US courts were asked to rule on the tort liability of the manufacturers of pacemakers and cochlear implants.

IoB devices also create legal uncertainty when addressing complex issues at the crossroads of IoB and criminal law. For example, it is not clear if the data feed generated by an IoB device connected to the brain can be qualified as "testimonial evidence" (Matwyshyn, 2019, p. 148) and should be treated with higher judicial scrutiny by courts. The third generation of IoB devices melded to the human brain will

undoubtedly impact traditional legal concepts of criminal law and criminal procedural law. In the era of IoB, law and ethics will be facing challenging dilemmas when non-conscious yet highly intelligent algorithms (Harari, 2017) may know us better than we know ourselves.

8 | CONCLUSION

By delineating some of the ethical and legal concerns regarding IoT and how it penetrates almost all aspects of human life, it is hoped that more emphasis be given to designing and creating a more responsible approach. Through such an approach, it is evident that not all ethical and legal issues may be resolved, but a pathway into a more balanced transition may be triggered. The cons of IoT may outweigh the pros greatly if such ethical concerns are overlooked and if legal issues are not addressed in a timely and appropriate way. In other words, at the pinnacle of technology and what it can offer to change the world as we know it, a sophisticated and responsible human intervention seems to stand out as the most sought-after virtue.

The IoT is here now in our lives. The IoB will become the new normal soon where human bodies and minds form a connected network of bodies pervaded by the Internet. The transition from IoT to IoB poses great potential for innovations and advancements and dangers and challenges. Legislators, policymakers, regulators, and consumer advocates bear the heavy burden of addressing the present challenges IoT raises. Public policy issues demand urgency and reactiveness from both the private and public actors. Because IoT is a global phenomenon, a coordinated global response is needed.

Such urgency is more pressing when we contemplate the awaiting challenges of a society pervaded by the IoB. When IoB becomes the new normal, privacy concerns and security flaws currently visible in the IoT might directly and physically threaten the integrity and the safety of the human body. Scholars will have to redefine the relationship between the code and the human. The integrity of human bodies will rely more and more on the Internet and its infrastructure. In this context, the future calls for a balance between divergent interests of technological IoT advancements, IoB innovations, and human safety.

ENDNOTES

[1] *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 133 S. Ct. 1,138 (2013).

[2] *Clapper*, 568 U.S. at 409.

[3] The *Clapper* decision created a circuit split among federal U.S. courts. For example, the Ninth Circuit in *Krottner v. Starbucks Corp*. (628 F.3d 1,139 (ninth Cir. 2010)) held that employees who establish a threat of real and imminent harm resulting from the theft of a laptop containing personal data have standing to claim remedies under state law. Conversely, the Third Circuit in *Reilly v. Ceridian Corp*. (664 F.3d 38 (3d Cir. 2011)) found that, despite the increased risk of identity theft, the plaintiffs are alleging a hypothetical and future injury and do not have standing to recover damages under Article III.

[4] Complaint before the U.S. District Court for the Northern District of California, *Simins v. Zoom Video Communications Inc*., Case No. 5:20-cv-02893.

[5] Complaint before the U.S. District Court Central District of California, *Todd Hurvitz v. Zoom Video Communications Inc*., et al., Case No. 2:20-cv-03400.

[6] Complaint before the U.S. District Court for the Northern District of California, *Robert Cullen v. Zoom Video Communications Inc*., Case No. 5:20-cv-02155; Complaint before the U.S. District Court for the Northern District of California, *Michael Drieu v. Zoom Video Communications Inc*., et al., Case No. 5:20-cv-02353.

REFERENCES

Botterman, M., & Tallacchini, M. (2018). Ethical design in the internet of things. *Science and Engineering Ethics*, *24*, 905–925.

Buttrick, H. G., Davidson, J., & McGowan, R. J. (2016). The skeleton of a data breach: The ethical and legal concerns. *Richmond Journal of Law and Technology*, *23*(1), 1–21.

Carey, S. (2018). Does Amazon Alexa or Google home listen to my conversations. https://www.techworld.com/security/does-amazon-alexa-listen-to-my-conversations-3661967/

Determann, L., & Fellmeth, A. X. (2001). Don't judge a sale by its license: Software transfers under the first sale doctrine in the United States and the European community. *University of San Francisco Law Review*, *36*(1), 1–107.

Elvy, S. -A. (2018). Commodifying consumer data in the era of the internet of things. *Boston College Law Review*, *59*(2), 424–522.

Fellmeth, A., & Kheschtchin-Kamel, A. (2019). The end of ownership. *Jurimetrics: The Journal of Law, Science & Technology*, *59*(3), 399–408.

Gilmore, G. (1974). *The death of contract*. Columbus: Ohio State University Press.

Guillemin, P., & Friessi, P. (2009). Internet of things strategic research roadmap. http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf.

Haller, S., Karnouskos, S., & Schroth, C. (2009). *The internet of things in an enterprise context*. Berlin Heidelberg: Springer.

Harari, Y. N. (2017). *Homo deus: A brief history of tomorrow*. New York, NY: HarperCollins Publishers.

Kirtley, J. E., & Memmel, S. (2018). Rewriting the "book of the machine": Regulatory and liability issues for the internet of things. *Minnesota Journal of Law, Science & Technology*, *19*(2), 455–513.

Kobayashi, G., Quilici-Gonzalez, M.E., Broens, M.C., & Quilici-Gonzalez, J. A. (2016). The ethical impact of the internet of things in social relationships. IEEE Consumer Electronics Magazine, July, 85–89.

Loewenthal, M. (2014). Internet of things: Current privacy policies don't work. https://www.informationweek.com/big-data/hardware-architectures/internet-of-things-current-privacy-policies-dont-work/a/d-id/1278925.

Matwyshyn, A. M. (2019). The internet of bodies. *William & Mary Law Review*, *61*(1), 77–167.

Meglio, M. (2020). Embracing insecurity: Harm reduction through a no-fault approach to consumer data breach litigation. *Boston College Law Review*, *61*(3), 1223–1269.

Nissenbaum, H. (2015). Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics*, *24*(3), 831–852.

Peppet, S. R. (2014). Regulating the internet of things: First steps toward managing discrimination, privacy, security, and consent. *Texas Law Review*, *93*(1), 85–178.

Perzanowshi, A., & Schultz, J. M. (2016). *The end of ownership: Personal property in the digital economy*. Cambridge, Massachusetts: The MIT Press.

Popescul, D., & Georgescu, M. (2013). Internet of things – Some ethical issues. *The USV Annals of Economics and Public Administration*, *13*, *2* (18), 208–214.

Rens, A. (2019). Who is in charge here? The internet of things, governance and the global intellectual property regime. *UCLA Journal of law & Technology*, *23*(2), 1–54.

Schultz, J. (2016). The internet of things we don't own? *Communications of the ACM*, *59*(5), 36–38. https://doi.org/10.1145/2903749

Schwartz, P. M. (2018). Legal access to the global cloud. *Columbia Law Review*, *118*(6), 1681–1762.

Siegel, J. (2020). When the internet of things flounders: Looking into Gdpr-esque security standards for IoT devices in the United States from the consumers' perspective. *Journal of High Technology Law*, *20* (1), 189–229.

Van den Hoven, J. (2013). Internet of things factsheet ethics. http://www.digitalchampion.bg/uploads/agenda/en/filepath_85.pdf

Weber, R. H. (2013). Internet of things – Governance quo vadis? *Computer Law and Security Review*, *29*(4), 341–347.

Zhilla, F., Abou Daher, L., Arikan, C. L., & El-Khoury, M. (2018). Conceptualizing the determinants of ethical decision making in business organizations. *Problems and Perspectives in Management*, *16*(4), 30–41.

AUTHOR BIOGRAPHIES

Moufid El-Khoury is a visiting lecturer in Law at Notre Dame University (NDU) - Lebanon. He taught law in France and Kuwait. He practises law in the Middle East and is admitted in New York State.

Cenk Lacin Arikan is an assistant professor at the American University of the Middle East (AUM). He is the Department Chair of Human Resource Management at the College of Business Administration. His research areas include Innovation, Strategy, Corporate Entrepreneurship, Corporate Culture, Business Ethics, and Family Businesses.

How to cite this article: El-Khoury M, Arikan CL. From the internet of things toward the internet of bodies: Ethical and legal considerations. *Strategic Change*. 2021;30:307–314. https://doi.org/10.1002/jsc.2411